



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,716	07/06/2001	Maurice Milgram	28944/37579	3971
4743	7590	06/21/2005	EXAMINER	
MARSHALL, GERSTEIN & BORUN LLP 233 S. WACKER DRIVE, SUITE 6300 SEARS TOWER CHICAGO, IL 60606			MOORTHY, ARAVIND K	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 06/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/900,716	MILGRAM, MAURICE
	Examiner	Art Unit
	Aravind K. Moorthy	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 28 December 2004.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-40 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) Claim(s) _____ is/are allowed.
6) Claim(s) 1-40 is/are rejected.
7) Claim(s) _____ is/are objected to.
8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 18 October 2001 is/are: a) accepted or b) objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
5) Notice of Informal Patent Application (PTO-152)
6) Other: _____.

DETAILED ACTION

1. Claims 1-40 are pending in the application.
2. Claims 1-40 have been rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. **Claims 1-13, 16-27 and 34-39 rejected under 35 U.S.C. 102(e) as being anticipated by Rosset et al U.S. Patent No. 6,704,715 B1.**

As to claim 1, Rosset et al discloses a security method using information transmission by light means between a user electronic apparatus having at least one input interface and a screen, and an electronic security device which comprises:

- a receive interface having at least one light sensor for receiving input information coming from the user electronic apparatus [column 5, lines 1-42];
- an emit interface adapted to emit output information as a function at least of received input information, the output information corresponding to a security code for communicating to the input interface of the user electronic apparatus [column 5, lines 1-42]; and
- an electronic central unit connected to the receive and emit interfaces and adapted to determine the output information as a function at least of the input

information and to cause the output information to be emitted by the emit interface [column 5, lines 1-42];

the security method comprising the following steps:

- a) causing the input information to be transmitted by the user electronic apparatus to the receive interface of the electronic security device [column 5 line 40 to column 6 line 57];
- b) causing the output information to be determined by the central unit of the electronic security device, as a function of the input information [column 5 line 40 to column 6 line 57];
- c) causing the emit interface of the electronic security device to emit the output information corresponding to the security code, and communicating the security code to the user electronic apparatus, via the input interface of the user electronic apparatus [column 5 line 40 to column 6 line 57]; and
- d) verifying that the security code received by the user electronic apparatus is related to the input information by a predetermined relationship [column 5 line 40 to column 6 line 57];

wherein during step a), the light sensor of the, electronic security device is placed facing the screen of the user electronic apparatus while the screen is caused to emit a modulated light signal carrying the input information [column 5 line 40 to column 6 line 57].

As to claim 2, Rosset et al discloses during step d), certain operations performed by means of the user electronic apparatus are authorized or not authorized as a function of verifying the security code [column 5 line 40 to column 6 line 57].

As to claim 3, Rosset et al discloses that the electronic security device belongs to a medium carrying digital data and readable by the user electronic apparatus [column 5 line 40 to column 6 line 57].

As to claim 4, Rosset et al discloses that the data medium used is an optical disk having an annular data area surrounding a central portion carrying no digital data, which central portion includes the light sensor [column 5 line 40 to column 6 line 57].

As to claim 5, Rosset et al discloses that during step a), the modulated light signal is emitted in a predetermined area belonging to the screen, and the light sensor of the data medium is placed in the immediate vicinity of the predetermined area [column 5, lines 1-42].

As to claim 6, Rosset et al discloses that during step a), the predetermined area of the screen is indicated by at least one mark displayed by the screen [column 5, lines 1-42].

As to claim 7, Rosset et al discloses that during step c), the output information is emitted by the electronic security device in the form of a sound signal [column 3 line 35 to column 4 line 7].

As to claim 8, Rosset et al discloses that the sound signal containing the output information is listened to by a human operator, which operator determines the security code as a function of the listened-to signal and communicates this security code to the user electronic apparatus via its input interface [column 3 line 35 to column 4 line 7].

As to claim 9, Rosset et al discloses that the sound signal containing the output information is received directly by the input interface of the user electronic apparatus [column 3 line 35 to column 4 line 7].

As to claim 10, Rosset et al discloses that the sound signal containing the output information is transmitted to a remote monitoring station which determines the security code as a function of the sound signal and transmits the security code to the input interface of the user electronic apparatus [column 3 line 35 to column 4 line 7].

As to claim 11, Rosset et al discloses that during step c), the output information is emitted by the electronic security device by being displayed on a display device [column 3 line 35 to column 4 line 7].

As to claim 12, Rosset et al discloses that encoded data is caused to be interchanged between a remote central station communicating with the user electronic apparatus and the central unit of the electronic security device via the emit and receive interfaces of the electronic security device [column 5 line 40 to column 6 line 57].

As to claim 13, Rosset et al discloses that the electronic security device stores a count of units of value, and the central unit of the electronic security device is adapted to cause the count of units of value to vary as a function of encoded data received and emitted by the central unit via the received and emit interface [column 6, lines 25-50].

As to claim 16, Rosset et al discloses a step of activating at least certain functions of the electronic security device, during which step a predetermined access code is communicated to the central unit of the electronic security device [column 6, lines 25-50].

As to claim 17, Rosset et al discloses that during the activation step, the access code is communicated to the central unit by means of a user-actuatable input interface of the electronic security device [column 3, lines 1-8].

As to claim 18, Rosset et al discloses that during the activation step, the access code is communicated to the central unit by positioning the light sensor of the electronic security device successively in register with a plurality of predetermined areas belonging to the screen of the user electronic apparatus. Rosset et al discloses the various predetermined areas of the screen emitting respective different predetermined optical signals, each corresponding to a symbol displayed on the screen.

As to claim 19, Rosset et al discloses that in order to communicate the access code to the central unit of the electronic security device, the access code is initially communicated to the user electronic apparatus using the input interface of the user electronic apparatus [column 5 line 40 to column 6 line 57]. Rosset et al discloses that the light sensor of the electronic security device is placed facing the screen of the user electronic apparatus [column 5 line 40 to column 6 line 57]. Rosset et al discloses that the screen is caused to emit a modulated light signal corresponding to the access code [column 5 line 40 to column 6 line 57].

As to claim 20, Rosset et al discloses that during step b), the central unit of the electronic security device is caused to determine the output information as a function of the input information and a personal code previously communicated to the central unit by the user of the electronic security device [column 5 line 40 to column 6 line 57].

As to claim 21, Rosset et al discloses that during step b), the personal code is communicated to the central unit of the electronic security device by means of a user-actuatable input interface of the electronic security device [column 3, lines 1-8].

As to claim 22, Rosset et al discloses that during step b), the personal code is communicated to the electronic central unit by positioning the light sensor of the electronic security device successively in register with a plurality of predetermined areas belonging to the screen of the user electronic apparatus, these various predetermined areas of the screen emitting respective different predetermined light signals and each corresponding to a symbol displayed on the screen [column 5 line 40 to column 6 line 57].

As to claim 23, Rosset et al discloses that during step b), to communicate the personal code to the central unit of the electronic security device [column 5 line 40 to column 6 line 57]. Rosset et al discloses that the personal code is initially communicated to the user electronic apparatus by using the input interface of the user electronic apparatus [column 5 line 40 to column 6 line 57]. Rosset et al discloses that the light sensor of the electronic security device is placed facing the screen of the electronic user apparatus. Rosset et al discloses that the screen is caused to emit a modulated light signal corresponding to the personal code [column 5 line 40 to column 6 line 57].

As to claim 24, Rosset et al discloses that during step d), a monetary operation is either authorized or not authorized [column 3, lines 9-12].

As to claim 25, Rosset et al discloses that the electronic security device stores at least one count of units of value, and during step d) an operation implying a change to the count of units of value is either authorized or not authorized [column 2, lines 31-62].

As to claim 26, Rosset et al discloses that during step d), units are exchanged between the count of units of value in the electronic security device and a remote count of units managed by a remote apparatus connected by telecommunications means to the user electronic apparatus [column 2, lines 31-62].

As to claim 27, Rosset et al discloses that during step d), after a count of units of value in the electronic security device has been modified [column 6 line 58 to column 7 line 32]. Rosset et al discloses that the output interface is caused to emit acknowledgment information [column 6 line 58 to column 7 line 32]. Rosset et al discloses that the acknowledgment information is communicated to the user electronic apparatus via the input interface of the user electronic apparatus [column 6 line 58 to column 7 line 32].

As to claim 34, Rosset et al discloses that the input information is transmitted between at least two emitting areas belonging to the screen of the user electronic apparatus and at least two light sensors belonging to the electronic security device [column 7 line 38 to column 8 line 39].

As to claim 35, Rosset et al discloses that the light signals received by the two light sensors are decoded by calculating a difference between the light signals [column 7 line 38 to column 8 line 39].

As to claim 36, Rosset et al discloses that a binary signal is determined by comparing the difference with a threshold value, and then the binary signal is processed by median filtering [column 7 line 38 to column 8 line 39].

As to claim 37, Rosset et al discloses that a binary signal is determined by comparing the difference with a threshold value previously determined by causing a predetermined calibration

signal to be transmitted between the emitting, areas of the screen and the light sensors [column 7 line 38 to column 8 line 39].

As to claim 38, Rosset et al discloses that one of the emitting areas of the screen emits a modulated light signal, while the other of the emitting areas emits a constant light signal [column 7 line 38 to column 8 line 39].

As to claim 39, Rosset et al discloses a disk comprising an annular data area surrounding a central portion carrying no digital data, the optical disk being readable by a user electronic apparatus by means of a light beam reader, which user electronic apparatus further comprises at least one input interface and a light emitting screen, the data medium including an electronic security device which comprises:

- a receive interface having a least one light sensor disposed in the central portion of the optical disk and adapted to receive input information coming from the screen of the user electronic apparatus [column 6 line 58 to column 7 line 32;]
- an emit interface adapted to emit output information as a function of received input information, the output information corresponding to a security code for communication to the input interface of the user electronic apparatus [column 6 line 58 to column 7 line 32; and]
- an electronic central unit connected to the receive and emit interfaces and adapted to determine the output information as a function of the input information and to cause the output information to be emitted by the emit interface [column 6 line 58 to column 7 line 32].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rosset et al U.S. Patent No. 6,704,715 B1 as applied to claim 1 above, and further in view of Yamaoka et al U.S. Patent No. 6,149,064.

As to claims 14 and 15, Rosset et al does not teach that the electronic security device belongs to a portable digital data medium which can be: read by the user electronic apparatus while the data medium is set in motion. Rosset et al does not teach the electronic security device storing at least one count of utilization units. Rosset et al does not teach the central unit of the security device causing the count to vary as a function of the movements of the data medium as detected by a motion sensor. Rosset et al does not teach that the utilization unit count is read by an external reader using a communication interface belonging to the security device.

Yamaoka et al teaches a portable digital data medium that can be: read by the user electronic apparatus while the data medium is set in motion [column 6 line 55 to column 7 line 42]. Yamaoka et al teaches the electronic security device storing at least one count of utilization units [column 6 line 55 to column 7 line 42]. Yamaoka et al teaches the central unit of the security device causing the count to vary as a function of the movements of the data medium as detected by a motion sensor [column 6 line 55 to column 7 line 42]. Yamaoka et al teaches that

the utilization unit count is read by an external reader using a communication interface belonging to the security device [column 6 line 55 to column 7 line 42].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rosset et al so that the card would have been read by an electronic apparatus while the card was in motion. The electronic security device would have stored at least one count of utilization units. The central unit of the security device would have caused the count to vary as a function of the movements of the data medium as detected by a motion sensor. Yamaoka et al teaches that the utilization unit count would have been read by an external reader using a communication interface belonging to the security device.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rosset et al by the teaching of Yamaoka et al because it provides an IC card reader that is able to easily and accurately position a contact carriage with respect to the card moving direction [column 2, lines 9-21].

5. Claims 28-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rosset et al U.S. Patent No. 6,704,715 B1 as applied to claim 20 above, and further in view of Takeda U.S. Patent No. 5,191,644.

As to claims 28 and 33, Rosset et al teaches that the light sensor of the electronic security device is placed facing the screen area selected by the user and the modulated light signal emitted by the screen area is picked up by means of the light sensor [column 5, lines 1-31]. Rosset et al teaches that during step d), the user's selection is confirmed as a function of verifying the security code received by the user electronic apparatus during step d) after modifying the count of units of value in the electronic security device [column 5, lines 1-31].

Rosset et al does not teach that the user is caused to select a screen area on the screen of the user electronic apparatus, and associated with predetermined visual signaling amongst a plurality of screen areas associated with different visual signaling, the screen areas emitting respective different modulated light signals carrying different input information. Rosset et al does not teach that the different screen areas are juxtaposed on the screen of the user electronic apparatus.

Takeda teaches that a user is caused to select a screen area on the screen of the user electronic apparatus, and associated with predetermined visual signaling amongst a plurality of screen areas associated with different visual signaling, the screen areas emitting respective different modulated light signals carrying different input information [column 5, lines 24-58]. Takeda teaches that the different screen areas are juxtaposed on the screen of the user electronic apparatus [column 6, lines 23-66].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rosset et al so that a user would have been caused to select a screen area on the screen of the user electronic apparatus. It would have been associated with predetermined visual signaling amongst a plurality of screen areas associated with different visual signaling. The screen areas would have emitted respective different modulated light signals carrying different input information. The different screen areas would have been juxtaposed on the screen of the user electronic apparatus.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rosset et al by the teaching of Takeda because it provides

a multi window control system that is capable of rapidly displaying those areas of overlapping windows which contain visible image information [column 2, lines 34-38].

As to claim 29, Rosset et al teaches that during step d), a count of votes is incremented corresponding to the selection made by the user during step a), and providing the selection is validated by verification of the security code [column 2, lines 31-62].

As to claim 30, Rosset et al teaches that the electronic security device stores information specifying previous elections in which the user of the electronic security device has participated, the information being updated by means of input information during step a), and during step b) or c), normal operation of the electronic security device is inhibited if the input information received for a new vote indicates that the user has already voted in this election [column 2, lines 31-62].

As to claim 31, Rosset et al teaches that during step d), the screen is caused to emit a modulated light signal carrying an acknowledgment signal confirming that the user's vote has been taken into account, and the participation information in the memory of the electronic security device is updated only when the light sensor of the electronic security device has received this acknowledgment signal [column 2, lines 31-62].

As to claim 32, Rosset et al teaches that the modulated light signals corresponding to different screen areas are modified in random manner after each vote cast by a user [Takeda column 5, lines 24-58].

6. Claims 40 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rosset et al U.S. Patent No. 6,704,715 B1 as applied to claim 39 above, and further in view of Yamaoka et al U.S. Patent No. 6,149,064.

As to claim 40, Rosset et al does not teach that the security device further includes a motion sensor.

Yamaoka et al teaches a security device that includes a motion sensor [column 6 line 55 to column 7 line 42].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rosset et al so that security device would have included a motion sensor.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rosset et al by the teaching of Yamaoka et al because it provides an IC card reader that is able to easily and accurately position a contact carriage with respect to the card moving direction [column 2, lines 9-21].

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
June 16, 2005

Ayaz Sheikh
AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100